Sign-in issues

Context

Google and Apple's businesses run on data and they are seeking to increase their control over end user data. They are looking to capture more data via sign-on and authentication by bundling such business-to-business functionality into their business-to-consumer software OS and browsers[1]. Through enabling their browser software to provide such services to end users the browser functionality substitutes for services currently provided by businesses across the world wide web.

Authentication is an essential step in effecting online payments and the increase of browser functionality centralises functions that have until now been decentralised and protected as part of the decentralised architecture of the web. The following steps are being taken together:

- User Authentication.
- Google's Privacy Sandbox (including Web ID aka single sign-on via the browser);[2]
- Apple's Intelligent Tracking Prevention (which has already enabled sign-in via Apple's browser).[3]
- W3C Payments API.[4]

Overall, Google and Apple are coordinating their positions on authentication and sign-in. They have jointly developed an authentication template and are working together on the WebID and on payments proposals.[5] All are designed to capture user data from to sign-in via the browser, instead of through decentralised systems[6] or sign-in using competing[7] sign-in systems and services.[8] The CMA identified this central issue of the control over user sign-in and competition for user sign-in data[9] in its report of 1 July 2020[10] with Appendix Z providing a detailed discussion of competition over personal identity management systems. We expect this issue to be prominent in the CMA's current browser Market Investigation.

Each of the platforms currently restricts competition between payment systems through their app store agreements and guidelines.[11] Technical restrictions on use that can prefer or default to Google Pay or Apple Pay at other points in the user journey can achieve an equivalent outcome. When considering

---

[1] As is exemplified by the recently implemented proposal to increased payments functionality via the browser and other proposals such as Web ID for single sign-on through the browser.

[2] See CMA Decision of 11.2.2022 at https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf. Google offered undertakings not to proceed with its Privacy Sandbox browser changes that would have the reduced the functionality and competitiveness of rival online advertising systems until it has created new tools that provide equivalent functionality to that which exists today. See e.g., para 5.20 "The Commitments will ensure that, if Google proceeds to removing TPCs, the Privacy Sandbox tools will be effective substitutes for the different forms of functionality provided by TPCs and other information deprecated by the Privacy Sandbox Proposals."

[3] See CNIL investigation at https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising-apples-implementation-att-framework-autorite-does-not-issue and EU investigations into Apple.

[4] See generally Web Payments Working Group https://www.w3.org/blog/wpwg/2022/05/16/web-payments-meeting-may-2022-edition/

[5] See Google's Web ID proposal that is part of its Privacy Sandbox: https://github.com/samuelgoto/WebID

[6] See for example services provided by businesses such as Net ID.

[7] https://uk.pcmag.com/migrated-46739-onlinecloud-backup-services/71363/the-best-identity-management-solutions-for-2020

[8] By contrast with the important work on standards to reduce friction in customer interactions such as password-less sign-in standards that are already supported in billions of devices with Cybersecurity authorities on increased security across a range of decentralised systems: https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins/

[9] See para 13 page 8, para 4.57 page 165, para 6.46 page 321 and how they gather consumer data at para 4.28 page 157 "Platforms receive and process data when consumers sign into an app or website using their sign in functionality, whereby consumers can securely sign into third-party apps without having to create, authenticate and remember new usernames and passwords. Sign in as an issue box 4.1 page 156 and data capture in Annex F of the CMA's report of 1 July 2020 (see Fn 12).

[10] https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf

[11] See CMA's market study into mobile ecosystems: final report summary: https://assets.publishing.service.gov.uk/media/62a228228fa8f50395c0a104/Final_report_summary_doc.pdf and the EU Commission case AT.40452 Apple – Mobile payments. Please also see Spotify's complaint at https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_1073/IP_20_1073_EN.pdf and Epic's complaint at https://www.epicgames.com/site/en-US/news/epic-games-files-eu-antitrust-complaint-against-apple.

their recently implemented W3C payments proposal, it is important to understand this context. If Google and Apple can obtain user sign-in via a joint template or via their browsers, they obtain competitive advantage over rivals who also need users to sign-in.

Payments, wallets, and the importance of authentication for online commerce

Online payments are used by people who have "online wallets". For those making payments online, setting up an online wallet entails the end user inserting payment card details into an online payments system. This differs from using a card reader (and sometimes adding a pin for double-factor authentication), as occurs in the offline world. Payment details are often inserted into website systems such as Amazon or any other online trading store.

Before accessing an online store to buy goods or services the website will ask the user for some information with which to authenticate the user is a human being, mainly to protect against fraud. To get sign-in to their platforms rather than into websites directly, Google and Apple have jointly created a single authentication template:

Figure 1 Online Authentication

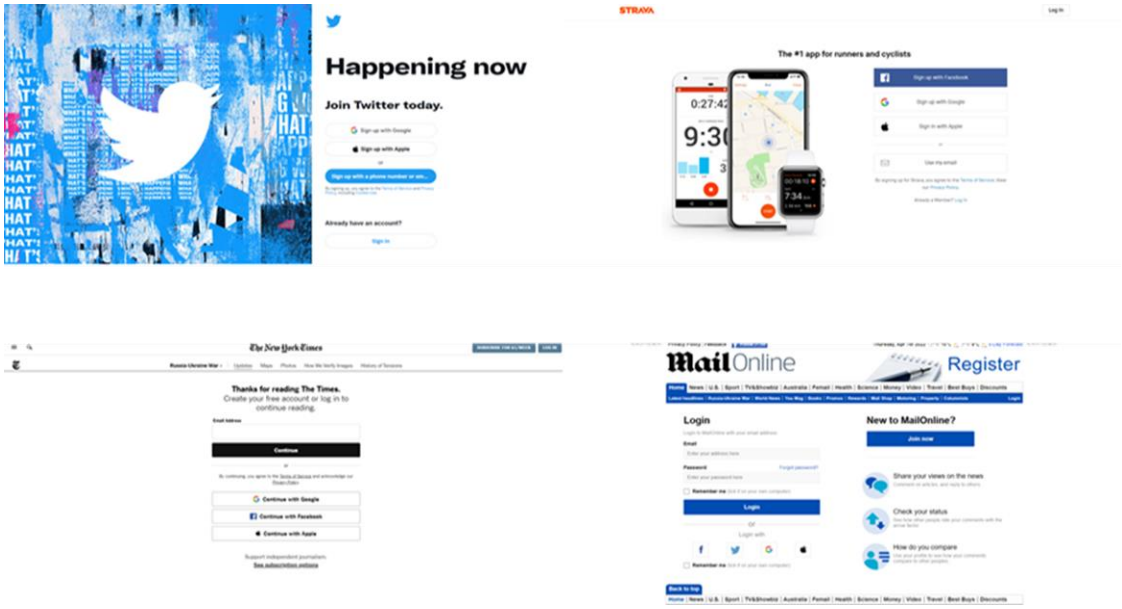

Figure 1 provides four different examples for authenticating the identity of the end user when accessing websites. The traditional, tried and tested mechanism of online commerce is for each user to sign into each website as and when needed. For example, the Mail Online, one of the world's most read English language newspapers online,[12] requires no authentication to visit the website. It is provided free of charge and is ad funded. Most news businesses (and most other websites) operate in a way that is frictionless to the user requiring no sign in or disclosure of identity in exchange for accessing digital content and services. In contrast, systems such as the New York Times use a form of sign-in which captures and processes users' identity, for which they must obtain consent on use of data, as well as send payment to the digital property if they wish to subscribe.

Figure 1 also illustrates that the joint authentication template is currently being used for sign-in to Twitter. Twitter presents Google and Apple at the top of the list of sign-in alternatives. As is well

[12] https://www.statista.com/statistics/246077/reach-of-selected-national-newspapers-in-the-uk

known, presentation and location in lists makes a difference to user preference[13]. It also puts Google and Apple in a powerful position. Specifically, when the user uses the Google or Apple authentication software to access each website, they are trading through Google or Apple and have accepted the position of Google or Apple as their gateway. As users are then already signed into Google or Apple, their identity-linked personal data is stored within the Google and Apple's systems- providing Google and Apple with data for mapping and advantages over their rivals, whenever that data can be used.

Online substitution[14] for online and offline payment systems: two sided markets can be integrated through platforms

Offline wallets are storage mechanisms for cards in the same way that online wallets are storage mechanisms for card details. However, one major difference is that to use an offline wallet there is no need to sign in or authenticate the end user before the wallet can be used. Physical possession normally suffices to indicate ownership that this is the user's wallet and payment method. The online wallet is different. Prior to the user sharing identity a business does not know their identity and thus authentication is needed to make such a disclosure.

Sign-in and sharing data is an essential step if a user is to use a payment system. In effect, following the authentication process outlined above, taken together with the further change proposed at the W3C to the browser, the risk is that an online wallet from which the user then chooses a payment card will be constrained and limited with inbuilt preference for Google Pay and Apple Pay. Moreover, the unilateral policies dictated by either internet gatekeeper could interfere with required interoperability among business-to-business transactions under the new Digital Markets Act.

Today, Google and Apple's authentication technology is deployed in many businesses' websites. Their payments systems technology competes with other online payments systems technology.[15] If Google and Apple can anti-competitively preference and discriminate in favour of their own systems and processes, competition and efficiency in the provision of payments products will suffer.

Markets and businesses affected

There is a market for authentication and sign-in. This is primarily affected by Google an Apple's joint authentication template and bundling of this authentication service into the browser and has been considered in detail by the CMA.[16]

Looking more closely at payments markets, businesses do not typically operate only online or only offline. As a result, they will operate both payments systems for both physical and online stores. When looking at the effects on markets it is thus important to appreciate that those effects will not be limited to online payments markets.

Well-known brands involved in both offline and online and integrated website offerings include[17]: PayPal, Square, Oracle, Sage, Clover, Zettle, Just Giving, Enthuse, Checkout.com, Birdeye, Freshbooks, GoCardless Venmo, and Stripe.

---

[13] See Google Search Shopping where ranking on SERP is known to be preferred by customers and see further for CMA work on "Dark Patterns" where choice screen and nudge architecture such as the template is used to corral and influence user choices.

[14] Guidelines on market analysis and the assessment of significant market power under the EU regulatory framework for electronic communications networks and services (Text with EEA relevance) 2018/C 159/01

[15] As provided by businesses such as Charity Checkout.

[16] In its investigation into Online Platforms and Digital Advertising the CMA reviewed in some detail in Annex Z the mechanisms through which competition might more effectively be assured. The central concern of that study related to how Google and Facebook combined and use data across markets. The CMA was particularly concerned about the use of data in digital advertising markets and expected that similar questions might arise in other markets where [dominant] firms are able to re-use data gathered from core user-facing activities. The CMA identified (at para 215 of Annex Z) as a potential solution the prospect that certain Personal Information Management Systems (or PIMS) exist which could help to address the issue. The CMA found, for example, at para "Finally, PIMS may facilitate a more formal value exchange involving the consumer. This could involve consumer-side monetisation, with flows of micropayments from publishers and platforms to consumers in exchange for access to their data." PIMS are likely to highly relevant to remedies in relation to the current UK Market Investigation concerning mobile browsers.

[17] https://www.g2.com/products/checkout-com/competitors/alternatives

Software that is affected would include that which provides payments gateway software from businesses such as Bolt.com, Ebiz Charge, Authorize.net, Payoneer, Razorpay, Paytm Business.

There is currently a thriving and competitive market with the "Top 50" suppliers including those that provide financial transaction software such as Oracle and Sage as well as a range of smaller fintech businesses. See for example: https://www.softwaresuggest.co.uk/checkout-com/alternatives.

All can be displaced by the tech platforms with the aid of their sign-in processes.

Self-Preference for Google Pay and Apple Pay

Google and Apple have an incentive to prefer their own products when offering digital wallets and payments technology. This provides them as platform owners with the benefit of linking the customer's authentication details with their payment details to capture the payment systems and software markets. Thus, part of the Google and Apple proposal is to ensure that their payment mechanism, Google Pay or Apple Pay, is preloaded and preferred in consumers' ***browser***. Google and Apple are looking to integrate payments within their Browsers such that they can be conducted and used with such ease that there is little scope for competition from alternative solutions.

As with the self-preference system that has been condemned by the Court of Justice in the Google Search (shopping) case, the proposal at W3C is for each alternative payment card to be listed in what is, in effect a ***browser wallet.*** Whereas rival digital wallets and Personal Information Management Systems (PIMS) must compete in the market for adoption, Apple and Google distribute their own PIMS in a manner reminiscent of how Microsoft displaced Netscape by bundling its own browser with the distribution of its operating system.

Currently each website owner such as the Mail Online in the example above, not only contracts with business solution provider but also with its customers on terms offered when customers visit and authenticate and sign-in to each website. Current contracts guarantee different things depending on the trading conditions under which transactions take place. Privacy commitments are made by each website that utilise end user personal data, whether higher risk situations when business providers use personal data linked to identity such as with authentication or payments or lower risk situations when business providers use personal data not linked to identity as with most consumer interactions with most digital properties. If Google and Apple are allowed to substitute the current contractual terms which exist in respect of each website with their own terms, which involve higher privacy risks to specific individuals, this, in effect, replaces and degrades the choices as well as the quality of privacy protection offered to consumers who are trading online.